What is Claimed Is:

1. A method for detecting and preventing security breaches in network traffic, the method comprising:

reassembling a plurality of TCP packets in the network traffic into a TCP stream;

inspecting the TCP stream to detect information indicative of security breaches;

dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches; and

forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of security breaches.

2. The method of claim 1, wherein inspecting the TCP stream to detect information indicative of security breaches comprises inspecting the TCP stream for protocol irregularities.

3. The method of claim 1, wherein inspecting the TCP stream to detect information indicative of security breaches comprises searching the TCP stream for attack signatures.

4. The method of claim 3, wherein searching the TCP stream for attack signatures comprises using stateful signature detection.

5. The method of claim 1, wherein inspecting the TCP stream to detect information indicative of

security breaches comprises using a plurality of network intrusion detection methods.

6. The method of claim 5, wherein the plurality of network intrusion detection methods comprises at least protocol anomaly detection.

7. The method of claim 5, wherein the plurality of network intrusion detection methods comprises at least signature detection.

8. The method of claim 1, further comprising grouping the plurality of TCP packets into packet flows and sessions.

9. The method of claim 1, further comprising storing the packet flows in packet flow descriptors.

10. The method of claim 9, further comprising searching the packet flow descriptors for traffic signatures.

11. The method of claim 9, wherein inspecting the TCP stream comprises searching for a network attack identifier in the TCP stream based on the packet flow descriptors and sessions associated with the TCP stream.

12. The method of claim 11, wherein the network attack identifier comprises a protocol irregularity.

13. The method of claim 11, wherein the network attack identifier comprises an attack signature.

14. The method of claim 11, wherein the network attack identifier comprises a plurality of network attack identifiers.

15. The method of claim 14, wherein the plurality of network attack identifiers comprises at least a protocol irregularity.

16. The method of claim 14, wherein the plurality of network attack identifiers comprises at least an attack signature.

17. The method of claim 13, wherein the attack signatures and the traffic signatures are stored in a signatures database.

18. The method of claim 8, wherein grouping the plurality of TCP packets into packet flows and sessions comprises storing the packet flows and sessions in a hash table.

19. The method of claim 18, wherein storing the packet flows and sessions in a hash table comprises computing a hash value from a 5-tuple consisting of: a source IP address; a destination IP address; a source port; a destination port; and a protocol type.

20. The method of claim 2, wherein inspecting the TCP stream for protocol irregularities comprises:

storing a plurality of protocol specifications supported by the network in a protocol database; and

querying the protocol database to determine whether the plurality of TCP packets in the packet flows

and sessions are compliant with one or more of the plurality of protocol specifications in the protocol database.

21. The method of claim 3, wherein searching the TCP stream for attack signatures comprises querying the signatures database to determine whether there are matching signatures in the TCP stream.

22. The method of claim 21, wherein determining whether there are matching signatures in the TCP stream comprises using DFA for pattern matching.

23. The method of claim 1, further comprising reconstructing the plurality of TCP packets from a plurality of packet fragments.

24. A system for detecting and preventing security breaches in network traffic, the system comprising:

a TCP reassembly software module for reassembling a plurality of TCP packets in the network traffic into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of security breaches;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches; and

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of security breaches.

25. The system of claim 24, further comprising an IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets.

26. The system of claim 24, further comprising a flow manager software module for grouping the plurality of TCP packets into packet flows and sessions.

27. The system of claim 26, wherein the flow manager software module comprises a routine for storing the packet flows and sessions into a hash table.

28. The system of claim 27, wherein the routine for storing the packet flows and sessions into a hash table comprises a routine for storing the packet flows in packet flow descriptors.

29. The system of claim 27, wherein the routine for storing the packet flows and sessions into a hash table comprises a routine for computing a hash value from a 5-tuple consisting of: a source IP address; a destination IP address; a source port; a destination port; and a protocol type.

30. The system of claim 24, wherein the software module for inspecting the TCP stream to detect information indicative of security breaches comprises a protocol anomaly detection software module.

31. The system of claim 24, wherein the software module for inspecting the TCP stream to detect

information indicative of security breaches comprises a stateful signature detection software module.

32. The system of claim 28, further comprising a traffic signature detection software module for searching the packet flow descriptors for traffic signatures.

33. The system of claim 24, wherein the software module for inspecting the TCP stream for information indicative of security breaches comprises a plurality of software modules.

34. The system of claim 33, wherein the pluralify of software modules comprises at least a protocol anomaly detection software module.

35. The system of claim 33, wherein the plurality of software modules comprises at least a stateful signature detection software module.

36. The system of claim 34, wherein the protocol anomaly detection software module comprises:

a routine for storing a plurality of protocol specifications supported by the network in a protocol database; and

a routine for querying the protocol database to determine whether the plurality of TCP packets in the packet flows and sessions are compliant with one or more of the plurality of protocol specifications in the protocol database.

37. The system of claim 36, wherein the protocol specifications comprise specifications of one or more of: TCP protocol; HTTP protocol; SMTP protocol; FTP protocol; NETBIOS protocol; IMAP protocol; POP3 protocol; TELNET protocol; IRC protocol; RSH protocol; REXEC protocol; and RCMD protocol.

38. The system of claim 35, wherein the stateful signature detection software module comprises a routine for querying a signatures database to determine whether there are matching attack signatures in the TCP stream.

39. The system of claim 38, wherein the routine comprises using DFA for pattern matching.

40. The system of claim 24, further comprising:

a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream;

a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented;

a routine for distributing the network security policy to one or more gateway points in the network; and

a routine for updating the protocol database and the signatures database.

41. The system of claim 24, further comprising a graphical user interface comprising:

a routine for displaying network security information to network security administrators; and

a routine for specifying a network security policy.

42. A system for detecting and preventing security breaches in network traffic, the system comprising:

a network intrusion detection and prevention sensor placed in a network gateway, wherein the network intrusion detection and prevention sensor comprises:

a routine for reassembling a plurality of TCP packets into a TCP stream;

a software module for inspecting the TCP stream to detect information indicative of security breaches;

a software module for dropping a TCP packet from the TCP stream if the TCP stream contains information indicative of security breaches; and

a software module for forwarding a TCP packet from the TCP stream to a network destination if the TCP stream does not contain information indicative of security breaches;

a central management server to control the network intrusion detection and prevention sensor; and

a graphical user interface for configuring the network intrusion detection and prevention sensor.

43. The system of claim 42, wherein the network intrusion detection and prevention sensor is placed inside a firewall.

44. The system of claim 42, wherein the network intrusion detection and prevention sensor is placed outside a firewall.

45. The system of claim 42, wherein the network intrusion detection and prevention sensor further comprises an IP defragmentation software module for reconstructing a plurality of packet fragments into the plurality of TCP packets.

46. The system of claim 42, wherein the network intrusion detection and prevention sensor further comprises an IP router software module for routing a TCP packet from the TCP stream if the TCP stream does not contain information indicative of network security breaches through the network.

47. The system of claim 42, wherein the network intrusion detection and prevention sensor further comprises a flow manager software module for grouping the plurality of packets into packet flows and sessions.

48. The system of claim 47, wherein the flow manager software module comprises a routine for storing the packet flows in packet flow descriptors.

49. The system of claim 42, wherein the software module for inspecting information indicative of security breaches comprises a protocol anomaly detection software module.

50. The system of claim 42, wherein the software module for inspecting information indicative of

security breaches comprises a stateful signature detection software module.

51. The system of claim 48, further comprising a traffic signature detection software module for searching the packet flow descriptors for traffic signatures.

52. The system of claim 42, wherein the software module for inspecting information indicative of security breaches comprises a plurality of software modules.

53. The system of claim 52, wherein the plurality of software modules comprises at least a protocol anomaly detection software module.

54. The system of claim 52, wherein the plurality of software modules comprises at least a stateful signature detection software module.

55. The system of claim 42, wherein the central management server comprises:

a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream;

a routine for storing a network security policy identifying the network traffic to inspect and a plurality of network attacks to be detected and prevented; and

a routine for distributing the network security policy to the network intrusion detection and prevention sensor.

56. The system of claim 42, wherein the graphical user interface comprises:

a routine for displaying network security information to network security administrators;

a routine for displaying status information on the network intrusion detection and prevention sensor; and

a routine for specifying a network security policy.

57. A network intrusion detection and prevention sensor for detecting and preventing network security breaches at a network gateway, the network intrusion detection and prevention sensor comprising:

a flow manager software module for grouping a plurality of packets into packet flows and sessions;

a TCP reassembly software module for reassembling a plurality of TCP packets from the plurality of packets into a TCP stream;

a software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of security breaches;

a software module for dropping a packet from the plurality of packets if the TCP stream contains information indicative of security breaches; and

a software module for forwarding a packet from the plurality of packets to a network destination if the TCP stream does not contain information indicative of security breaches.

58. The network intrusion detection and prevention sensor of claim 57, further comprising an IP defragmentation software module for reconstructing a

plurality of packet fragments into the plurality of TCP packets.

59. The network intrusion detection and prevention sensor of claim 57, wherein the network intrusion detection and prevention sensor further comprises an IP router software module for routing a TCP packet from the TCP stream if the TCP stream does not contain information indicative of network security breaches through the network.

60. The network intrusion detection and prevention sensor of claim 57, wherein the network intrusion detection and prevention sensor is controlled by a network security policy specifying the network traffic to inspect and a plurality of network attacks to be detected and prevented.

61. The network intrusion detection and prevention sensor of claim 60, wherein the network security policy is defined by a network security administrator using a graphical user interface.

62. The network intrusion detection and prevention sensor of claim 57, wherein the graphical user interface comprises:

a routine for displaying network security information to network security administrators;

a routine for displaying status information on the network intrusion detection and prevention sensor; and

a routine for specifying the network security policy.

63. The network intrusion detection and prevention sensor of claim 60, wherein the security policy is stored and distributed to the network intrusion detection and prevention sensor by a central management server.

64. The network intrusion detection and prevention sensor of claim 63, wherein the central management server comprises a routine for collecting a plurality of security logs and alarms recording information about security breaches found in the TCP stream.

65. The network intrusion detection and prevention sensor of claim 57, wherein the software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of security breaches comprises a protocol anomaly detection software module.

66. The network intrusion detection and prevention sensor of claim 57, wherein the software module for inspecting the TCP stream according to the packet flows and sessions to detect information indicative of security breaches comprises a stateful signature detection software module.

67. The network intrusion detection and prevention sensor of claim 58, wherein the software module for inspecting the plurality of packets according to the packet flows and sessions to detect information indicative of security breaches comprises a plurality of software modules.

68. The network intrusion detection and prevention sensor of claim 67, wherein the plurality of software modules comprises at least a protocol anomaly detection software module.

69. The network intrusion detection and prevention sensor of claim 67, wherein the plurality of software modules comprises at least a stateful signature detection software module.